Build Your Human Firewall - One Smart Step at a Time

Why This Roadmap Exists

Cybersecurity doesn't fail because businesses don't care — it fails because it feels overwhelming.

This roadmap breaks cybersecurity into **12 vital actions**, one per month. Each step is practical, achievable, and proven to reduce real-world risk for small businesses.

Think of this as **building a Human Firewall** — strong people, supported by smart technology, making safer decisions every day.

2026 Roadmap: https://actsmartit.com/2026-roadmap)

January— *Set Up MFA Everywhere!* (ACTSmartIT.com/january-mfa)
February— *Secure and Test Backups* (ACTSmartIT.com/february-backup)

Coming Up:

March—Security Awareness Training

April—Phishing & Email Security

May—Passwords & Password Managers

June—Device security

July—Mobile Device Security

August—Data Protection & Encryption

September—Ransomware Awareness & Response

October—Cybersecurity Awareness Month

November—Safe Browsing & Online Scams

December—Incident Response & "What To Do If…"

ACT SMART I.T.
Helping You Benefit From Today's Technologies

332 Main Street, Wareham, MA 02571
781-826-9665 | 855-WOW-SERVICE
ACTSmartIT.com

Your 12 Month Cybersecurity Roadmap

Follow us each month at:
ACTSmartIT.com/2026-roadmap/

February's Vital Action: Backups That Actually Work

Because a backup you've never tested is just a hope.

Cyberattacks, ransomware, hardware failures, and human mistakes happen every day. The businesses that recover fastest all have one thing in common: **working, tested backups.**

This month's vital action is making sure your backups can actually save you when it matters most.

What Should Be Backed Up?

If it matters to your business, it needs a backup.

At a minimum, back up:

- ✔ Business documents & shared files
- ✔ Accounting & financial data
- ✔ Email & cloud data (Microsoft 365, Google Workspace)
- ✔ Databases & line-of-business applications
- ✔ Servers, systems, and critical configurations
- ✔

👉 *If losing it would stop work, cost money, or cause panic—back it up.*

How Often Backups Should Run?

Backups should match how often your data changes.

Best practice for most businesses—the 3-2-1 Backup Rule:

3 Copies of Data: The original production data plus at least two backup copies.

2 Different Media Types: Store backups on different, separate systems to avoid single-point failure (e.g., one on a local NAS, one on an external USB drive, or in the cloud)

1 Off-site Copy: Keep at least one backup in a geographically different, secure location, such as a different building, a secured, off-site, or a cloud service.

👉 *Manual backups are unreliable.* ***Automation matters.***

Why Testing Restores Matters

Backups aren't useful unless they can be restored.

Many businesses discover too late that:

- Backups were incomplete
- Files were corrupted
- Restores were never tested
- Data couldn't be recovered fast enough

Vital action:

- Test restores regularly
- Confirm files open and systems run
- Know *how long* recovery actually takes

👉 *A backup that can't be restored is the same as no backup at all.*

How Backups Beat Ransomware

Ransomware wants one thing: **your only copy of your data.**

When you have secure, tested backups:

- You don't have to pay the ransom
- You can restore clean data
- Downtime is minimized
- A disaster becomes a bad day—not a business-ending event

👉 *Backups turn criminals into inconveniences.*

February Action Step

Ask this one question:

> ***"If our data disappeared today, could we restore it—and how long would it take?"***

If the answer isn't clear, this month's vital action is simple:

Review, verify, and test your backups.

https://actsmartit.com/february-backup/